Embodiments of the invention may also restrict certain users, or certain categories of users, in the type of image data that may be reviewed. This may be done in exemplary embodiments by limiting access to image and/or transaction data selectively to users, based on the types of triggering events associated with the storage of images. Alternatively, certain users may be precluded from viewing images captured from certain cameras. This capability may be used to prevent certain users from observing certain images such as images which may include customer PINs or the combination to a lock on an ATM. By preventing selected users from accessing certain image data based on the type of triggering event or camera associated therewith, images captured by the system that need not be restricted may be made available more broadly and used for potentially more purposes.

Detailed Description Text (117):
In system 328, device 330 is connected to one or more automated banking machines schematically indicated 332. Automated banking machine 332 is similar to the machines previously discussed and includes a plurality of transaction function devices. Automated banking machine 332 may have one or more cameras or other image capture devices adjacent thereto as represented by camera 334. As will be appreciated, a number of cameras may be positioned adjacent to the machine by being within and/or near to automated banking machine 332 for purposes of capturing image data related to users, documents, surroundings or other types of visual inputs that may be desirable to capture and analyze. Camera 334 is operatively connected to device 330 such that device 330 may receive and capture image data therefrom. It should be understood that additional types of data capture devices may also be included adjacent to or within automated banking machine 332. This may include for example microphones for capturing sound or voice information as well as devices which capture data related to transactions. Embodiments of the present invention can use voice recognition software to detect sounds from the microphone representative of words or the stress levels of sounds emanating from persons near the automatic banking machine. Such voice or sound data may be used in combination with images or other data to further detect and evaluate conditions at or near the automated banking machine. The data or information which is captured is also communicated to the device 30 through one or more appropriate electronic connections schematically indicated 336.

Previous Doc Next Doc Go to Doc#

L9: Entry 10 of 11 File: USPT Jun 24, 2003

DOCUMENT-IDENTIFIER: US 6583813 B1
TITLE: System and method for capturing and searching image data associated with transactions

Drawing Description Text (8):
FIG. 8 is a schematic view of the operation of the logical components of an embodiment of the invention responding to loss of usable video from a camera.

Drawing Description Text (51):
FIG. 53 is an exemplary screen presented at a user terminal associated with programming a sequence for detecting lack of usable video from a camera in which a camera is selected.

Detailed Description Text (15):
The operation of exemplary embodiments of the invention are further described with regard to the interaction of logical components of the system described in connection with FIGS. 3 through 9. It should be understood that the logical components are generally combinations of software and hardware used in carrying out the described functions. As shown in FIG. 3 the input signals from the cameras, microphones or other input devices are input to the device switching controller component 66. The device switching controller component in embodiments of the invention may include several components. The switching controller delivers signals, which in the described exemplary embodiment are analog signals, selectively in response to a record acquisition control component 68. The record acquisition 68 component receives hard and soft trigger signals including signals which control or otherwise indicate the operation of the transaction function devices in the automated banking machine or other signals which are used as an indicator to initiate a sequence of actions. The record acquisition component executes the instructions which indicate which image signals are desirable to process and record in response to the trigger signals. The record acquisition component further includes or works in connection with stored instructions, which are operative to detect conditions such as loss of usable video from a camera or other input device, and to begin acquisition of data from other devices in response thereto.

Detailed Description Text (46):
A further example may be used in connection with a banking machine which includes check accepting or other document accepting devices where the authenticity of the inserted document may require verification. The timing/sequence component may work in connection with an imaging device within the automated banking machine to capture an image of indicia on the inserted document, and to transmit an image of the document while the transaction is ongoing to a verification terminal in the network. Such a document may be viewed at such a terminal and/or electronically analyzed to compare the image of the document to verification information such as a handwriting or signature database for purposes of determining authenticity. The destination where such messages are sent may be varied depending on the nature and/or amount of the document, the time of day and other parameters depending on the instructions associated with the timing/sequence logic component 124.

Detailed Description Text (108):

L9: Entry 9 of 11 File: USPT Feb 8, 2005

DOCUMENT-IDENTIFIER: US 6853739 B2
TITLE: Identity verification system

Brief Summary Text (10):
Furthermore, secured access into restricted areas typically has little or no identity verification at all. A person wishing to enter a door, boom or turnstile presents a token or identification card to a data input device near the door, boom or turnstile. The data is sent back to the server controlling the access control system. The access control system checks a database of the access control server to verify that the token is valid or that the person associated with the identification card is authorized to enter the door, boom or turnstile. If the number on the token or identification card is authorized, the access control system will instruct, via electronic means, a magnetic lock or other locking mechanism that controls the door, boom or turnstile to release the lock and allow access to the person seeking entry. There is typically no visual verification of the person entering by an operator.

Brief Summary Text (18):
Still yet another aspect of the present invention is an identity verification system, the verification system comprising: (a) a plurality of referenced data input devices wherein each referenced data input device is associated with a data identification code; (b) a plurality of cameras for recording photographic images, wherein each camera is associated with a camera identification code; (c) a display means for displaying information to a system operator; (d) a communication control device remote from the data input devices, the cameras and the display means, said communication control device including (i) a camera server having a video engine in communication with at least one camera, wherein the video engine selectably captures a set of photographic images taken with the camera and converts the images into a compressed digital file linked to the camera identification code, a first data conversion engine in communication with at least one data input device, wherein the first data conversion engine captures a set of input data from the data input device and formats the captured data into a network protocol standard linked to the data identification code, and a second data conversion engine, wherein the second data conversion engine formats a set of output data for communication with the display means; and (ii) a main board that connects the camera server to the camera, the data input device, the display means and a computer network; (e) a plurality of keycatcher units; (f) a plurality of interactive local communication stations, each communication station comprising (i) a local central processing unit, (ii) a keyboard, and (iii) a monitor; and (g) at least one system central processing unit remote from the communication control device and in direct communication with the communication control device having (i) an installed biometric recognition system, (ii) a first processor means for generating a biometric template from the captured biometric data using the installed biometric recognition system, (iii) a second processor means for comparing and scoring the correspondence of two biometric templates using the biometric recognition system; (iv) storage means for storing a set of biometric templates in a biometric database, and (iv) searching means for searching the biometric database for a stored biometric template linked with an identifying parameter.

Brief Summary Text (21):

Yet another aspect of the present invention is a face recognition based method for verifying the identity of an individual, the method comprising the steps of: entering an identifier associated with a person through a referenced data input device into a communication control device, said communication control device in communication with a CPU; searching an enrolled face database residing on the CPU for the person's identifier, wherein said enrolled face database links a set of stored digitized facial template files of a number of individuals with a set of identifiers for each of the individuals; activating a camera reference-linked to the referenced data input device; gathering a plurality of photographic images of the person; capturing a set of selected photographic images with the communication control device and generating a set of compressed digitized image files from the selected photographic images; transmitting the compressed digitized image files to the CPU; processing the compressed digitized image files though a face recognition system residing on the CPU to form a test facial template file; comparing the test facial template file with the stored facial template file associated with the person's identifier in the face database; and providing feedback on the correspondence of the test facial template file with the stored facial template file to a visual output device associated with the biometric data entry mechanism.

Detailed Description Text (2):
The present invention relates to a security system that utilizes a biometrics recognition system (including but not limited to a face, fingerprint, hand or iris recognition system) to verify the identification of a person seeking authorization to enter a restricted area or to complete a restricted transaction. The system is described herein with reference to the Figures, in which like elements are referred to by like numerals.

Detailed Description Text (3):
A general schematic of a preferred embodiment of the present invention is illustrated in FIG. 2. In contrast to current passenger check-in terminals or verification points in sensitive access restricted areas, the present invention incorporates an objective biometric recognition system, such as a face recognition system, linked to one or more personal identifiers such as a passport number, a national identity document, a bank account number, an employee number, or other unique identification numbers.

Detailed Description Text (11):
The data input station 20 will also include at least one data input device 24. The data input device 24 may be any type of data input or data capture device, such as a magnetic card swipe reader, proximity sensor, check reader, barcode scanner, smart card reader, passport scanner, barcode scanner or even a biometrics input device such as a fingerprint scanner, hand geometry reader or microphone. Such devices are commercially available and are well known to one skilled in the art. One example of a usable magnetic strip reader is an Elk Card Reader, model number A10190 that is commercially available from Brush Industries, Sunbury, Pa.

Detailed Description Text (16):
Preferably the communication control device 28 has an Ethernet camera or video server device 30, such as is commercially available from Axis Communications of Lund, Sweden and an interconnecting main board 38, as is commercially available from BioCom, LLC of Houston, Tex. The particular camera server device 30, shown in FIG. 3, includes four composite video inputs, two RS232 input connectors and one RS485 input connector. The camera server device 30 is used in the present invention in cooperation with hardware that performs connecting functions and protocol conversion functions, as well as power distribution functions.

CLAIMS:

24. An identity verification system, the verification system comprising: (a) a plurality of referenced data input devices wherein each referenced data input

device is associated with a data identification code; (b) a plurality of cameras for recording photographic images, wherein each camera is associated with a camera identification code; (c) a display means for displaying information to a system operator; (d) a communication control device remote from the data input devices, the cameras and the display means, said communication control device including (i) a camera server having a video engine in communication with at least one camera, wherein the video engine selectably captures a set of photographic images taken with the camera and converts the images into a compressed digital file linked to the camera identification code, a first data conversion engine in communication with at least one data input device, wherein the first data conversion engine captures a set of input data from the data input device and formats the captured data into a network protocol standard linked to the data identification code, and a second data conversion engine, wherein the second data conversion engine formats a set of output data for communication with the display means; and (ii) a main board that connects the camera server to the camera, the data input device, the display means and a computer network. (e) a plurality of keycatcher units; (f) a plurality of interactive local communication stations, each communication station comprising (i) a local central processing unit, (ii) a keyboard, and (iii) a monitor; and (g) at least one system central processing unit remote from the communication control device and in direct communication with the communication control device having (i) an installed biometric recognition system, (ii) a first processor means for generating a biometric template from the captured biometric data using the installed biometric recognition system, (iii) a second processor means for comparing and scoring the correspondence of two biometric templates using the biometric recognition system; (iv) storage means for storing a set of biometric templates in a biometric database, and (iv) searching means for searching the biometric database for a stored biometric template linked with an identifying parameter.

Previous Doc Next Doc Go to Doc#